An Extension of $(2, m(m+1)/2)$-Threshold Secret Sharing Schemes

Yuji Suga(✉)

Internet Initiative Japan Inc., Iidabashi Grand Bloom,
2-10-2, Chiyoda-ku, Fujimi 102-0071, Japan
suga@iij.ad.jp

Abstract. Fast (k, n)-threshold secret sharing schemes with XOR operations have proposed by Kurihara et al. and Fujii et al. independently. Their method are ideal that share size is equal to the size of the data to be distributed with the benefits that can be handled very fast for using the only XOR operations at distribution and reconstruction processes. In these cases for the number of shares n, target data must be equally divided into individual $n_p - 1$ pieces where n_p is a prime more than n. The existing methods described above are configured using the cyclic matrices with prime order. On the other hand, a new method in WAIS2013 has proposed, this leads to general constructions of $(2, p+1)$-threshold secret sharing schemes. Moreover, we use m-dimensional vector spaces over $\mathbb{Z}_2$ on having bases that meet certain conditions in order to construct proposed methods. Moreover, existences of $(2, 2^m)$-threshold secret sharing schemes are published (in NBiS2013) by using a new notion "2-propagation bases set" as a bases set in m-dimensional vector spaces over $\mathbb{Z}_2$. However this construction for all parameter m is wrong, in other words, it constitutes just only $(2, m(m+1)/2)$-SSS, not $(2, 2^m)$-SSS. This paper corrects mistakes of construction and also proposes an accurate construction by using Galois field $GF(2^m)$ that elements are represented in the ring $F_p[X]/f(X)$ where f(X) is an irreducible polynomial, these functionalities lead to general constructions of $(2, 2^m)$-threshold secret sharing schemes.

1 Introduction

This paper describes new constructions of (2, n)-threshold secret sharing schemes using exclusive-OR operations and also shows their advantages. To indicate that proposed methods are suitable for use in cloud computing, this section introduces security challenges in the cloud environment.

1.1 Requirements in Use of Clouds

Many organizations are currently discussing the definition and standardization of cloud computing [1–5]. For example, the Open Cloud Manifesto states the key

© Springer International Publishing AG 2018
L. Barolli et al. (eds.), *Advances in Network-based Information Systems*,
Lecture Notes on Data Engineering and Communications Technologies 7,
DOI 10.1007/978-3-319-65521-5_84

characteristics of the cloud as the ability to scale and provision computing power dynamically in a cost efficient way and the ability of the consumer to make the most of that power without having to manage the underlying complexity of the technology [6].

By type of use cases, clouds can be classified into private or public cloud. Public cloud provided in open network has been recognized as an evolution version of the hosting services. On the other hand, there is also use in a closed network within companies/organizations, called private cloud. In the private cloud, customers can place under the control of servers, network devices and their own data. This means that customers have to design configurations of secure network and care various attacks and vulnerabilities of their own servers, so they also need server management costs. These types of clouds are used in accordance with the importance of the data to be treated. Here a lot of customers have a big concern: can we use various cloud services securely?

Using public cloud means entrusting the cloud providers with the management and processing of various business data. SAS 70 type II [7] is one of endorsement system for "cloud service provider's reliability". The Cloud Security Alliance also launched an initiative to encourage transparency of security practices within cloud providers [8]. Cloud Computing Use Case Discussion Group published a useful whitepaper related to SLA(Service Level Agreement) [9]. These activities give us a sense of safety when using public clouds, however operators in information systems department can not be relieved because technical components used in clouds are unclear. In particular, requirements for the confidentiality should be clear. For example one of suspicious questions is "what kind of cryptographic algorithms are used in this cloud environment?".

In this paper, we discuss about enterprise/system requirements in case of deployments of security/cryptographic technologies, especially cloud storage solutions with secret sharing schemes. Needs of secret sharing schemes are derived from privacy concerns by private/enterprise use cases, for example we feel skeptical to deposit our sensitive/private data to may-be-untrusted cloud services. Note that this paper does not describe other than CIA (confidentiality, integrity, availability) requirements, there are some other issues on the cloud environment, for example topics related to boundaries and digital forensics [10].

1.1.1 Secret Sharing Schemes

Secret sharing schemes [11,12] has been recognized as a technology that has a good balance confidentiality and availability requirements. As simplest example is (k, n)-threshold secret sharing scheme: A dealer gives a set of n shares from a secret, only when any group of t shares are gathered a secret would be reconstructed, but from $k-1$ pieces of shares they can not obtain any information about the secret.

The effects of the application of SSS are balancing of risk for leakage (Not all are exposed even if some leakage) and diversification of risk for loss (can be restored even if some are lose), SSS has flexibility that can be selected parameters n and k depending on the applications and the use cases.

1.1.2 Business Requirements in Use of SSS

Movements to provide secret sharing services in cloud environment are actually seen, however we can not see technical background and promise in the service from public press releases. Because of vulnerable system configurations and illegal cloud suppliers, there's a possibility that the customer information can be restored. So, in deployments of secret sharing schemes in cloud storage, we have to consider new proprietary system requirements: **confidentiality** in the data flow and **lightweight processing** in the distribution/recovery phases.

When a cloud provider replicates customer's data into different cloud providers (in Fig. 1), one of providers MAY obtain the qualified sets unintentionally. So we require transparency of data flow (details in next section) and also confidentiality of distributed data, that is we need fast secret sharing schemes.

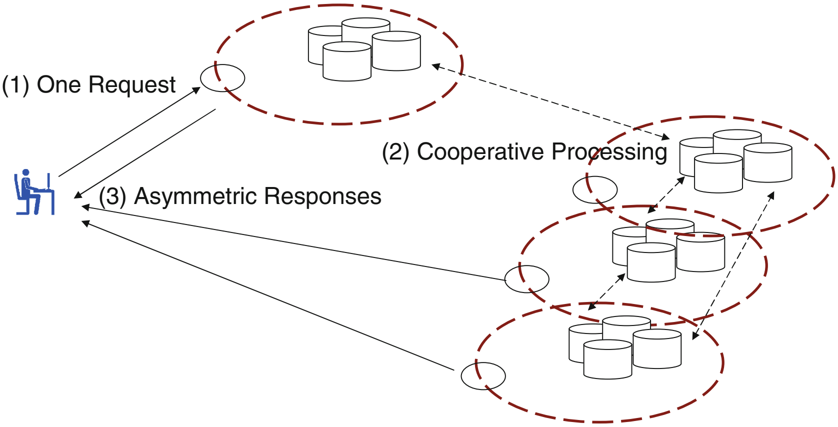

Fig. 1. Asymmetric cloud services

It assumes the case where the cloud providers archive data from the customer and process the data according to customer's requests, especially such as backup systems with low frequency of use. This paper propose secret sharing schemes "that coexist with the encryption process" suitable for use in the clouds.

1.2 Challenges to Be Solved

Let us consider the phase that replication, encryption and recovery of multiple pieces of customer data are repeated. It is considered generally that performing "recovery and decryption" by going back to the above-described data flow diagram. However a service may not be symmetric such as Fig. 1, that is a receiver and a responder may be different. Providing business model that gives the user a best option is desired, for example, in order to select preferentially from cloud services in view of the network topology, the route more efficient to transfer and lowest charging.

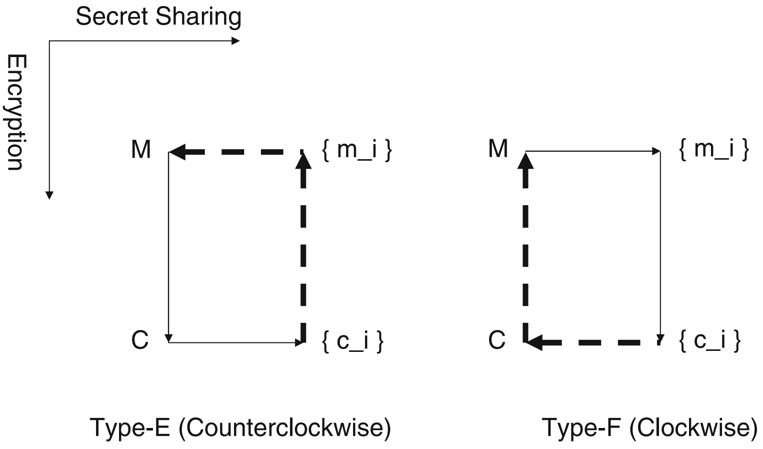

Fig. 2. The recovery process in Type-E, Type-F

This integrated services, we need common standard API and data format and also "commutative property of distributed processing and data encryption secret" as a new requirements in processing level such as Fig. 2. This paper has been investigated whether can be realized by using homomorphic functions, however we consider the prior to processing speed, so studied the fast method using exclusive-OR operations.

In this case, we know that encryption process and secret sharing distribution process are commutative by using stream cipher or block cipher encryption with the CTR mode as the encryption phase. So now we focus on previous secret sharing schemes using exclusive-OR operations.

1.3 Secret Sharing Schemes Using Exclusive-OR Operations

The (k, n)-threshold secret sharing schemes using exclusive-OR operations (XOR-(k, n)-SSS) are proposed by Fujii et al. [13,14] and Kurihara et al. [15–17] independently. A simple example XOR-(2, 3)-SSS described in [13] is as follows: Let a secret M be $M = M_1 || M_2$ $(M_1, M_2 \in \{0,1\}^d)$, $M_0 \in \{0\}^d$ (a d-bit zero binary) and we generate d-bit binaries R_0, R_1 randomly. Let shares $W_i (i = 0, 1, 2)$ be

- $W_0 = (M_0 \oplus R_0) \; || \; (M_2 \oplus R_1)$
- $W_1 = (M_1 \oplus R_0) \; || \; (M_0 \oplus R_1)$
- $W_2 = (M_2 \oplus R_0) \; || \; (M_1 \oplus R_1)$

where $||$ denotes a concatenation of binary data, $\oplus$ denotes a bit-wise exclusive-OR operation.

For general (k, n)-threshold secret sharing scheme, a secret $M \in \{0,1\}^{d(n_p-1)}$ needs to be divided into $n^{'} := n_p - 1$ blocks $M_1, \ldots, M_{n_p-1} \in \{0,1\}^d$ where n_p is a prime such that $n_p \geq n$, and d is the bit-size of every divided block of the secret. In the above example, it satisfies that $n = n_p = 3$, the number of pieces of block is $n^{'} = n_p - 1 = 2$.

In order to describe above equations simply, we introduce a notation as follows:

W_0	W_{00}	$\ldots$	$W_{0n''}$
W_1	W_{10}	$\ldots$	$W_{1n''}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$
W_i	W_{i0}	$\ldots$	$W_{in''}$
$\ldots$	$\ldots$	$\ldots$	$\ldots$
W_n	W_{n0}	$\ldots$	$W_{nn''}$

where the number of pieces of blocks $n^{'} := n_p - 1$, $n^{''} := n^{'} - 1$ and $W_i = W_{i0} \;||\; \ldots \;||\; W_{in''}$ for any $i(i = 0, \ldots, n^{'})$,.

The previous XOR-(2, 3)-SSS can be also described as follows:

W_0	$M_0 \oplus R_0$	$M_2 \oplus R_1$
W_1	$M_1 \oplus R_0$	$M_0 \oplus R_1$
W_2	$M_2 \oplus R_0$	$M_1 \oplus R_1$

where $n = n_p = 3$, the number of pieces of blocks $n^{'} := n_p - 1 = 2$.

Note that these schemes are ideal secret sharing schemes similar to Shamir's SSS that every bit-size of shares equals bit-size of a secret. Kurihara et al. reported that their scheme performs the operations 900-hold faster than Shamir's SSS for the parameters $(k, n) = (3, 11)$ [16].

1.4 The Contrubutions of This Paper

In this section thgis paper shows that the existing secret sharing scheme using exclusive OR operations (XOR-SSS) is suitable for use in the clouds and introduces previous 2-out-of-n secret schemes by only using XOR operations. In next section, this paper proposes new methods of XOR-SSS and corrects mistakes of construction and also proposes an accurate construction by using Galois field $GF(2^m)$ that elements are represented in the ring $F_p[X]/f(X)$ where f(X) is an irreducible polynomial, these functionalities lead to general constructions of $(2, 2^m)$-threshold secret sharing schemes.

2 Reconsideration of XOR-$(2, n)$-SSS

2.1 Existing Examples of XOR-$(2, n)$-SSS as a Starting Point

In this subsection, constructions of XOR-$(2, n)$-SSS with circulant permutation matrices are explained.

For given prime n_p, the following is a set of shares $\{W_i\}$ of XOR-(2,n)-SSS with $n^{'} = n_p - 1$ such that $n = n_p$. $W_i(i = 0, \ldots, n-1) =$

$W_{i0} \mid\mid \dots \mid\mid W_{ij} \mid\mid \dots \mid\mid W_{in''}$ $(j = 0, \dots, n'' := n' - 1)$. Let a secret be $M = M_1 \mid\mid \dots \mid\mid M_{n'}$ where $M_1, \dots, M_{n'} \in \{0,1\}^d$, $M_0 \in \{0\}^d$ and d-bit binaries $R_0, \dots, R_{n''}$ be generated randomly. And let W_{ij} be $M_j \oplus R_{(j-i) \bmod n_p}$. For $n_p = 3$, a concrete construction of XOR-$(2,3)$-SSS with $n' = 2$ is as follows:

Example 1 (XOR-$(2,3)$-SSS [15]). $M = M_1 \mid\mid M_2$ $(n' = 2), M_0 \in \{0\}^d$

W_0	$M_0 \oplus R_0$	$M_1 \oplus R_1$
W_1	$M_2 \oplus R_0$	$M_0 \oplus R_1$
W_2	$M_1 \oplus R_0$	$M_2 \oplus R_1$

Moreover for $n_p = 5$, a concrete construction of XOR-$(2,5)$-SSS with $n' = 4$ is as follows:

Example 2 (XOR-$(2,5)$-SSS [15])

W_0	$M_0 \oplus R_0$	$M_1 \oplus R_1$	$M_2 \oplus R_2$	$M_3 \oplus R_3$
W_1	$M_4 \oplus R_0$	$M_0 \oplus R_1$	$M_1 \oplus R_2$	$M_2 \oplus R_3$
W_2	$M_3 \oplus R_0$	$M_4 \oplus R_1$	$M_0 \oplus R_2$	$M_1 \oplus R_3$
W_3	$M_2 \oplus R_0$	$M_3 \oplus R_1$	$M_4 \oplus R_2$	$M_0 \oplus R_3$
W_4	$M_1 \oplus R_0$	$M_2 \oplus R_1$	$M_3 \oplus R_2$	$M_4 \oplus R_3$

2.2 A New Method Proposed in WAIS2013

In WAIS2013, a new method have proposed, this leads to general constructions of $(2, p+1)$-threshold secret sharing schemes using only exclusive-OR operations with the same assumption of previous XOR-(k,n)-SSS. Let n' be the number of pieces of blocks, previous schemes [14,16] have a restriction about n', that is n' must equal $n_p - 1$ for a certain prime n_p. For example, XOR-(2,4)-SSS with $n' = 3$ must be used part of shares from XOR-(2,5)-SSS with $n' = 4$.

For given prime n_p, the following is a set of shares $\{W_i\}$ of XOR-(2,n)-SSS with $n' = n_p - 1$ such that $n = n_p + 1$. $W_i (i = 0, \dots, n-1) = W_{i0} \mid\mid \dots \mid\mid W_{ij} \mid\mid \dots \mid\mid W_{in''}$ $(j = 0, \dots, n'' := n' - 1)$. Let a secret be $M = M_1 \mid\mid \dots \mid\mid M_{n'}$ where $M_1, \dots, M_{n'} \in \{0,1\}^d$, $M_0 \in \{0\}^d$ and d-bit binaries $R_0, \dots, R_{n''}$ be generated randomly.

- $W_{00} = R_0$
- $W_{0j} = M_1 \oplus M_{j+1} \oplus R_j \quad (j = 1, \dots, n' - 1)$
- $W_{10} = M_1 \oplus R_0$
- $W_{1j} = W_{0,j-1} \oplus R_{j-1} \oplus R_j$
  $(j = 1, \dots, n' - 1)$
- $W_{ij} = W_{i-1,j-1} \oplus R_{j-1} \oplus R_j$
  $(i = 2, \dots, n' - 1, j = 1, \dots, n' - 1)$
- $W_{n',j} = M_2 \ \oplus, \dots, \oplus \ M_{n'} \oplus R_j$
  $(j = 1, \dots, n' - 1)$

The following new concrete distribution method proposed in WAIS2013 is XOR-$(2,4)$-SSS with $n^{'} = 2 \neq n - 1 = 3$.

Example 3 (XOR-$(2,4)$-SSS [18]). $M = M_1 || \ M_2$ $(n^{'} = 2), M_0 \in \{0\}^d$

W_0	$M_0 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1$
W_1	$M_1 \oplus M_2 \oplus R_0$	$M_1 \oplus R_1$
W_2	$M_1 \oplus R_0$	$M_0 \oplus R_1$
W_3	$M_2 \oplus R_0$	$M_2 \oplus R_1$

Now we consider a not-strictly-defined function $F()$. When we input distinct two shares, $F()$ outputs the data to be recovered in each part. For example, $F(\{W_0, W_1\}) = \{W_{00} \oplus W_{10}, W_{01} \oplus W_{11}\} = \{M_1 \oplus M_2, M_2\}$ in the above XOR-$(2,4)$-SSS, so we can obtain both M_1 and M_2 finally. Similarly,

- $F(\{W_0, W_2\}) = \{M_1, M_1 \oplus M_2\}$,
- $F(\{W_0, W_3\}) = \{M_2, M_1\}$,
- $F(\{W_1, W_2\}) = \{M_2, M_1\}$,
- $F(\{W_1, W_3\}) = \{M_1, M_1 \oplus M_2\}$,
- $F(\{W_2, W_3\}) = \{M_1 \oplus M_2, M_2\}$.

In any combinations of shares, we can observe obtaining both M_1 and M_2.

Moreover for $n_p = 5$, a concrete construction of XOR-$(2,6)$-SSS with $n^{'} = 4$ is as follows:

Example 4 (XOR-$(2,6)$-SSS [18])

W_0	$M_0 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1$	$M_1 \oplus M_3 \oplus R_2$	$M_1 \oplus M_4 \oplus R_3$
W_1	$M_1 \oplus R_0$	$M_0 \oplus R_1$	$M_1 \oplus M_2 \oplus R_2$	$M_1 \oplus M_3 \oplus R_3$
W_2	$M_1 \oplus M_4 \oplus R_0$	$M_1 \oplus R_1$	$M_0 \oplus R_2$	$M_1 \oplus M_2 \oplus R_3$
W_3	$M_1 \oplus M_3 \oplus R_0$	$M_1 \oplus M_4 \oplus R_1$	$M_1 \oplus R_2$	$M_0 \oplus R_3$
W_4	$M_1 \oplus M_2 \oplus R_0$	$M_1 \oplus M_3 \oplus R_1$	$M_1 \oplus M_4 \oplus R_2$	$M_1 \oplus R_3$
W_5	$M_{234} \oplus R_0$	$M_{234} \oplus R_1$	$M_{234} \oplus R_2$	$M_{234} \oplus R_3$

where $M_{234} := M_2 \oplus M_3 \oplus M_4$.

2.3 Introduction of a Concept "isomorphism" in XOR-$(2, n)$-SSS

For a matrix representation $\{W_{ij}\}$, we define the isomorphism in XOR-$(2, n)$-SSS as follows:

Definition 5 (Isomorphism in XOR-$(2, n)$-SSS). For an XOR-$(2, n)$-SSS Ψ with matrix-representation of W_{ij}, an XOR-$(2, n)$-SSS generated from the following operations is isomorphic to Ψ.

1. Replace a line with some other line.
2. Replace a column with some other column.
3. For all sub-shares of a column, add same data with XOR-operations.

From Example 1 we can obtain the next modified XOR-SSS.

Example 6 (A modification of Example 1)

W_0	$M_0 \oplus R_0$	$M_0 \oplus R_1$
W_1	$M_2 \oplus R_0$	$M_1 \oplus R_1$
W_2	$M_1 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1$

In order to observe relevances to Example 1, we modify Example 3.

Example 7 (A modification of Example 3)

W_0	$M_0 \oplus R_0$	$M_0 \oplus R_1$
W_1	$M_1 \oplus M_2 \oplus R_0$	$M_2 \oplus R_1$
W_2	$M_1 \oplus R_0$	$M_1 \oplus M_2 \oplus R_1$
W_3	$M_2 \oplus R_0$	$M_1 \oplus R_1$

Now we compare Examples 6 and 7, Example 7 is a extension of Example 6 because W_1 is added in Example 7.

Next we introduce another representation of XOR-$(2, n)$-SSS instead of matrix-representation. W_{ij} is represented by an element of $\mathbb{Z}_2^{n'}$, that is, when $W_{ij} = \bigoplus_{t=1}^{n'} \alpha_t M_t$, set $w_{ij} be (\alpha_1, \ldots, \alpha_{n'}) \in \mathbb{Z}_2^{n'}$.

The following case is a vector-representation of Example 6.

Example 8 (a vector-representation of Example 7)

W_0	$(0, 0)$	$(0, 0)$
W_1	$(1, 1)$	$(0, 1)$
W_2	$(1, 0)$	$(1, 1)$
W_3	$(0, 1)$	$(1, 0)$

2.4 Definition of 2-Propagation Bases Set and Constructions of XOR-$(2, m(m+1)/2)$-SSS

In a vector-representation Example 8, we can see that column vectors construct an n'-dimension vector space, for example it satisfies that $w_{10} = w_{20} + w_{30}$, $w_{11} = w_{21} + w_{31}$ where $+$ is add operation over $\mathbb{Z}_2^m$.

Definition 9 (2-propagation bases set). 2-propagation bases set $\{b_i\}(i = 1, \ldots, l)$ is a set of bases over $\mathbb{Z}_2^m$ satisfies the following properties: b_1 is a set of m zero-vectors and for all distinct two bases b_i, b_j, $b_i + b_j$ is also a basis over $\mathbb{Z}_2^m$.

Lemma 10. *The order of 2-propagation bases set $\{b_i\}$ over $\mathbb{Z}_2^m$ is presented as 2^t (optimal case: 2^m). A set $\{b_i\}$ has t generator bases $\{c_i\}(i = 1, \ldots, t)$, for all b_i it satisfies that $b_i = \sum_{j=1}^{t} \alpha_j c_j$.*

Theorem 11. *When an optimal 2-propagation bases set $\{b_i\}$ $(i = 1, \ldots, 2^m)$ over $\mathbb{Z}_2^m$, these exists an XOR-$(2, m(m+1)/2)$-SSS with vector-representation $\{w_{ij} = b_i^j\}$ $(i = 1, \ldots, 2^m$, $i = 1, \ldots, m)$.*

Proof. From the definition of 2-propagation bases set, for distinct u, v, $b_u + b_v$ is a basis, so $w_1^* = w_{u1} + w_{v1}, \ldots, w_m^* = w_{um} + w_{vm}$ are bases over $\mathbb{Z}_2^m$. The l-th element of $W_u \oplus W_v$ equals $\bigoplus_{s=1}^{m} w_l^{*(s)} M_s$. In this case, these exist m linearly independent simultaneous equations for $M_s (s = 1, \ldots, m)$, so we can reconstruct all M_s. □

Theorem 11 indicates the existence of 2-propagation bases sets is important, so the following program was implemented in order to show the existence of XOR-$(2, 2^m)$-SSS for small m.

Program.

1. set $m > 1$.
2. set $b_1 := \{(0, \ldots, 0), \ldots, (0, \ldots, 0)\}$.
3. set $b_2 := \{(1, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, \ldots, 1)\}$.
4. set c:= 3
5. $b_c{}^R{}_{\in}(\mathbb{Z}_2^m)^m$, check $rank(B_c + B_i)$ =?=m for all $i = 1, \ldots, c-1$
6. if YES then add b_c into $\{b_i\}$, set $c = c + 1$
7. if NO then return (5)

Here are some concrete examples of 2-propagation bases sets for small order. Note that W_0 corresponds to the zero vector bases and $W_1, \ldots, W_m$ are generator bases $c_i$related to Lemma 10. All shares are constructed by $\bigoplus_{s=1}^{m} w_l^{*(s)} M_s$ mentioned in Theorem 11.

Example 12 (*$m = 4$*: **XOR-**$(2, 4 \cdot 5/2)$**-SSS** [19])

W_0	$(0,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$	$(0,0,0,0)$
W_1	$(1,0,0,0)$	$(0,1,0,0)$	$(0,0,1,0)$	$(0,0,0,1)$
W_2	$(1,1,0,0)$	$(1,0,0,0)$	$(0,0,1,1)$	$(0,0,1,0)$
W_3	$(0,0,1,1)$	$(1,0,0,1)$	$(0,1,1,0)$	$(0,1,0,0)$
W_4	$(0,1,0,1)$	$(0,1,1,0)$	$(1,1,0,0)$	$(1,0,0,0)$
$W_1 + W_2$				
$W_1 + W_3$				
$W_1 + W_4$				
$W_2 + W_3$				
$W_2 + W_4$				

2.5 New Construction of XOR-$(2, m^2)$-SSS

The following example is a starting point of this subsection, this is leaded by previous work in a empirical program for parameter $m = 3$. This example is unexpectedly generated because a share $W_1 + W_2 + W_3$ is "the eighth" share. So this paper analyze the algerbraic interpretation of this example and as a result we could find construction for any parameters $m > 4$.

Example 13 **(**$m = 3$: **XOR-**$(2, 2^3)$**-SSS** [19]**)**

W_0	$(0,0,0)$	$(0,0,0)$	$(0,0,0)$
W_1	$(1,0,0)$	$(0,1,0)$	$(0,0,1)$
W_2	$(0,1,1)$	$(1,0,0)$	$(0,1,0)$
W_3	$(1,1,0)$	$(0,1,1)$	$(1,0,0)$
$W_1 + W_2$			
$W_1 + W_3$			
$W_2 + W_3$			
$W_1 + W_2 + W_3$	$(0,0,1)$	$(1,0,1)$	$(1,1,1)$

Each m-dimension vectors can be expressed by a element of Galois field $GF(2^m)$, so we attempt the previous example could be rewritten:

Let an irreducible polynomial $f(X)$ in $GF(2^3)$ be $X^3 + X + 1$, so we consider the field of 8 elements defined by $\mathbb{F}_{2^3} = F_2[X]/f(X)$. In this field, there are 8 elements: $0, 1, \alpha, \alpha^2, \ldots, \alpha^7$ where *alpha* is a primitive element in $\mathbb{F}_{2^3}$. All non-zero elements are follows:

- $\alpha^1 = \alpha^2 \cdot 0 + \alpha \cdot 1 + 1 \cdot 0$
- $\alpha^2 = \alpha^2 \cdot 1 + \alpha \cdot 0 + 1 \cdot 0$
- $\alpha^3 = \alpha^2 \cdot 0 + \alpha \cdot 1 + 1 \cdot 1$ (due to $\alpha^3 = \alpha + 1$)
- $\alpha^4 = \alpha^2 \cdot 1 + \alpha \cdot 1 + 1 \cdot 0$
- $\alpha^5 = \alpha^2 \cdot 1 + \alpha \cdot 1 + 1 \cdot 1$
- $\alpha^6 = \alpha^2 \cdot 1 + \alpha \cdot 0 + 1 \cdot 1$
- $\alpha^7 = \alpha^2 \cdot 0 + \alpha \cdot 0 + 1 \cdot 1$

So we archeive and rewrite the previous example as follows:

Example 14 **(**$m = 3$: **XOR-**$(2, 2^3)$**-SSS by using expression of a primitive element** *alpha***)**

W_0	0	0	0
W_1	α^2	α^1	α^0
W_2	α^3	α^2	α^1
W_3	α^4	α^3	α^2
$W_1 + W_2$	α^5	α^4	α^3
$W_1 + W_3$	α^6	α^5	α^4
$W_2 + W_3$	α^0	α^6	α^5
$W_1 + W_2 + W_3$	α^1	α^0	α^6

This expression is caused by the equation: $\alpha^i + \alpha^{i+1} = \alpha^{i+3}$ because the left hand is $\alpha^i(\alpha + 1)$, so we can apply $\alpha^3 = \alpha + 1$.

In the general case for parameter $m > 3$, there exists an irreducible polynomial formd by $X^m + X + 1$ in $\mathbb{F}_{2^m}$, so this fact implies gurantee of existense of XOR-$(2, 2^m)$-SSS for some parameters m (for instance, $m = 2, 3, 4, 6, 7, 9, 15$).

3 Conclusions and Future Work

For a set of basis over $\mathbb{Z}_2^m$, this paper introduces a concept "2-propagation bases set" and previous constructions of $(2, m(m+1)/2)$-threshold secret sharing schemes using exclusive-OR operations. This paper corrects mistakes of construction and also proposes an accurate construction by using Galois field $GF(2^m)$ that elements are represented in the ring $F_p[X]/f(X)$ where f(X) is an irreducible polynomial, these functionalities lead to general constructions of $(2, 2^m)$-threshold secret sharing schemes. In the future we need to extend proposals to the cases with $k \geq 3$ with estimation of calculation costs.

References

1. Open Cloud Manifesto. http://www.opencloudmanifesto.org/
2. Open Cloud Consortium. http://www.opencloudconsortium.org/
3. Cloud Security Alliance. http://www.cloudsecurityalliance.org/
4. DMTF's Open Cloud Standards Incubator. http://www.dmtf.org/standards/cloud
5. NIST's definition of cloud computing. http://csrc.nist.gov/groups/SNS/cloud-computing/
6. http://www.opencloudmanifesto.org/opencloudmanifesto2.htm
7. American Institute of Certified Public Accountants (AICPA), Statement on Auditing Standards (SAS) No. 70 type II. http://www.sas70.com/
8. Cloud Security Alliance: Security, Trust & Assurance Registry (STAR). https://cloudsecurityalliance.org/star/
9. Cloud Computing Use Case Discussion Group. Cloud Computing Use Case White Paper version 4. http://cloudusecases.org/
10. IIJ, IIR vol.4, Section 1.4.3: Cloud Computing and Security. http://www.iij.ad.jp/en/development/iir/pdf/iir_vol04_infra_EN.pdf
11. Shamir, A.: How to share a secret. Commun. ACM **22**(11), 612–613 (1979)
12. Blakley, G.R.: Safeguarding cryptographic keys. Proc. AFIPS **48**, 313–317 (1979)
13. Fujii, Y., Tada, M., Hosaka, N., Tochikubo, K., Kato, T.: A fast (2, n)-threshold scheme and its application. In: Proceedings of CSS2005, pp. 631–636 (2005). (in Japanese)
14. Tada, M., Fujii, Y., Hosaka, N., Tochikubo, K., Kato, T.: A secret sharing scheme with threshold 3. In: Proceedings of CSS2005, pp. 637–642 (2005). (in Japanese)
15. Kurihara, J., Kiyomoto, S., Fukushima, K., Tanaka, T.: On a fast (k, n)-threshold secret sharing scheme. IEICE Trans. Fund. **E91–A**(9), 2365–2378 (2008)
16. Kurihara, J., Kiyomoto, S., Fukushima, K., Tanaka, T.: A new (k, n)-threshold secret sharing scheme and its extension. In: 11th Information Security Conference (ISC2008). LNCS, vol. 5222, pp. 455–470 (2008)
17. Kurihara, J., Kiyomoto, S., Fukushima, K., Tanaka, T.: A fast (k, L, n)-threshold ramp secret sharing scheme. IEICE Trans. Fund. **E92–A**(8), 1808–1821 (2009)
18. Suga, Y.: New constructions of (2, n)-threshold secret sharing schemes using exclusive-or operations. In: The 7th International Workshop on Advances in Information Security (WAIS2013), pp. 837–842 (2013)
19. Suga, Y.: A fast (2 $2\hat{m}$)- threshold secret sharing scheme using M linearly independent binary vectors. In: The 6th International Conference on Network-Based information Systems (NBiS 2013), pp. 539–544 (2013)